

INTERNATIONAL SEARCH REPORT

Inte - final Application No
PC / IB2004/052259A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	<p>R. CRAMER, I.B. DAMGARD, J. B. NIELSEN: "Multiparty Computation from Threshold Homomorphic Encryption" BASIC RESEARCH IN COMPUTER SCIENCE, 'Online!' June 2000 (2000-06), pages 1-38, XP002319282 DENMARK ISSN: 0909-0878 Retrieved from the Internet: URL:http://citeseer.ist.psu.edu/cache/paper/cs/24589/http://zSzzSzwww.brics.dkzSzRSzSz00zSz14zSzBRICS-RS-00-14.pdf /cramer00multiParty.pdf> 'retrieved on 2005-02-25! page 3 - page 5 page 13 - page 32</p> <p>-----</p> <p style="text-align: center;">-/-</p>	1-9

 Further documents are listed in the continuation of box C. Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

Date of the actual completion of the international search

25 February 2005

Date of mailing of the international search report

10/03/2005

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax. (+31-70) 340-3016

Authorized officer

Apostolescu, R

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2004/052259

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 01/20562 A (VOTEHERE. NET; ADLER, JIM; GREEN, RICHARD, L; NEFF, C., ANDREW; DAI, W) 22 March 2001 (2001-03-22) page 15, line 3 – page 18, line 18 page 21, line 14 – page 24, line 4 -----	1-9
A	M. HIRT, K. SAKO: "Efficient Receipt-Free Voting Based or Homomorphic Encryption" EUROCRYPT 2000, 'Online! 2000, pages 1-18, XP002319283 SWITZERLAND Retrieved from the Internet: URL: http://citeseer.ist.psu.edu/cache/paper/cs/20658/ftp:zSzzSzftp.inf.ethz.chzSzpubzSzpublicationsSzpapersSzSzisczSzwwwisczSzHirSak00.pdf/hirt00efficient.pdf > 'retrieved on 2005-02-25! page 6 – page 13 -----	1-9
A	WO 03/077470 A (KONINKLIJKE PHILIPS ELECTRONICS N.V; TUYLS, PIM, T; KEVENAAR, THOMAS,) 18 September 2003 (2003-09-18) the whole document -----	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.
PCT/IB2004/052259

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
WO 0120562	A	22-03-2001		AU 3770200 A		17-04-2001
				AU 3922600 A		24-04-2001
				WO 0120562 A2		22-03-2001
				WO 0122200 A2		29-03-2001
				AT 243397 T		15-07-2003
				AU 3922700 A		17-04-2001
				CA 2382445 A1		22-03-2001
				DE 60003444 D1		24-07-2003
				DE 60003444 T2		06-05-2004
				DK 1224767 T3		13-10-2003
				EP 1224767 A2		24-07-2002
				ES 2200853 T3		16-03-2004
				JP 2003509727 T		11-03-2003
				PT 1224767 T		31-10-2003
				WO 0120431 A2		22-03-2001
				US 2002078358 A1		20-06-2002
WO 03077470	A	18-09-2003		AU 2003252817 A1		22-09-2003
				EP 1486027 A1		15-12-2004
				WO 03077470 A1		18-09-2003